the Availability Digest

www.availabilitydigest.com
@availabilitydig

Cyber Security and Downtime

Dr. Terry Critchley
May 2016

A few years ago, I wrote an article for the Availability Digest on Software Reliability, which comprised aspects of software and its development in aiding high availability of IT services:

Software Reliability Models: The Use of Defect Density as a Basis for the Prediction of Software Reliability
(http://www.availabilitydigest.com/public_articles/0808/software_reliability.pdf)

This paper is a follow-on from that journey into producing reliable software.

Review of Availability Numbers

The availability of a *service* can be defined by the end user as:

$$\text{Availability (A)} = \frac{\textit{Time it is functioning correctly}}{\textit{Time it is supposed to be functioning}} \times 100\ (\%)$$

$$\text{Non-availability (1 - A)} = \frac{\textit{Time it is functioning incorrectly}}{\textit{Time it is supposed to be functioning}} \times 100\ (\%)$$

Traditional thinking about high availability often confuses *system* availability with *service* availability. In a nutshell, *system availability* means that the hardware and software is working and no parts of it are down (not functioning); but this does not mean that the service, for example online orders, is fully available. In the case of software, it may be that it is functioning but not doing what it is supposed to be doing in the way the end user expects.

An example might be year-end processing. The program has been working as planned all year, but the year-end processing part has never been accessed in normal processing. When it put to use at the end of the year, the program is found to be running through its code but producing erroneous results for the users. The operations people will swear that everything is working fine, but to the end user it most certainly isn't. This is what I call a logical *outage* or *downtime*, of which there are many examples, some of which are covered in Reference 1.

Outage Causes

The causes of outages are as numerous as leaves on a tree, and include:

- hardware and software failures, either total or partial where only certain users are affected. This can be a blip or a disaster in which the whole system is blitzed out of action in some way.

- environmental events such as floods, lightning, overheating and numerous others.
- various logical outages.
- **cyber attacks or malware**

Cyber Attacks and Availability

The threat of cyber attacks is relatively new and was unheard of in the heady mainframe days of the 1970s and 1980s. It is here today and is rapidly on the increase, both numerically and with respect to damage potential and intensity.

Again, traditional thinking says that a cyber attack, although a nuisance, does not constitute an outage - a nuisance, yes, but not an outage. This is not borne out by experience, and there are numerous papers that have been published backing this inference up. They include a report to the IT advisory committee of the President of the United States. One of the papers I saw showed a 20-fold increase in cyber attacks between 1995 and 2005 (in the thousands), so you can imagine the numbers today. Targets for these attacks cover a wide spectrum and include:

- personal; your PC/tablet and mine.
- social media such as dating sites with a view to extortion or blackmail. Twitter has suffered from multiple attacks.
- finance systems with a view to obtaining money in some way.
- military and other government sites for espionage or sabotage purposes.

There are many types of cyber/malware attacks that arrive as new threats or as mutations of older ones to which an antidote has been developed. It is pointless to cover them all here, especially as I don't know them all. All I know is that many are disruptive and some quite malicious. The basic problems they might cause are:

- locking out further system access until a ransom is paid. An example is Ukash, which is now eliminated.
- flooding a site with fake traffic to cause it to slow down or shut down because of excessive load, such as a distributed denial of service (DDoS) attack.
- file encryption where, again, a ransom is demanded for the key to unlock the files. Examples are ransomware and variations.
- theft of data, particularly that of monetary value to the perpetrator(s) such as bank account details. Examples are botnets[1]. These attacks are often surreptitious and not immediately apparent and are especially persistent threats which reside on a system and spring into life every so often.
- destruction or alteration of data or metadata, such as indexes or system software.

Whatever the cause, the attack is likely to cause an outage or hiatus of some sort. Even the non-disruptive data theft will cause an outage since once detected, it is unlikely the site will continue operating as normal. A disaster recovery site may possibly be of no avail since it too may have duplicated dubious data from the primary system.

So, cyber attacks will almost certainly cause outages of variable durations which cannot be forecast. The solutions are beyond this paper (and most people too), but the fact of this article is to help recognize the impact on system and data availability of cyber attacks.

[1] Around the date of this paper (2010) it was estimated that botnets infected nearly 10 million systems.

Impact of Cyber Attacks

Firstly, some sites are reluctant to admit these sort of attacks for multiple reasons, not least of which is the fact that it advertises that *'we are open for illicit access, folks'*, a clarion call to the cyber thief. Secondly, it is often difficult to determine the scope of any damage caused by such attacks, the solution for recovery, and how to ensure it doesn't happen again.

The Preponderance of Cyber Attacks

A survey outlined in reference 3[2]. shows the following responses from respondents:

- 26% reported that the attack had a serious or sustained impact on IT networks with some effect on operations.
- 23% reported that the attack had effects on operations, causing reputational damage[3] or service interruption.
- 12% reported that the attack had a serious sustained effect on operations, such as environmental damage, floods etc.
- 4% reported that the attack cause a 'critical breakdown' in operations.

The survey asked the correspondents to estimate the costs of such outages, and they came up with an average figure for a 24 hour outage of $6.3 m. These are big bucks in anybody's language.

Reference 4. below, appropriately called '*Victimology,*' reported that businesses reported almost 324,000 hours of downtime due to some form of cybercrime, though I'm not sure of the sample size. Either way, it's a big number.

Other Impacts

These attacks are not confined to certain industries' enterprise systems. They include data centers, disaster recovery sites, and even industrial control systems that monitor and control a number of industrial facilities. These include military and public utility control systems. There have been recent incidents involving electric grid systems, notably one in the Ukraine, covered in the Availability Digest article:

How The Ukraine Power Grid Was Hacked
http://www.availabilitydigest.com/public_articles/1103/ukraine_outage.pdf

and the other article referenced in it. The outcome of such attacks goes far beyond just financial loss, as you might imagine.

The Solution?
Solving this problem taxes greater minds than mine, but foolproof solutions evade us though there are many partial solutions and solution specifications around. The biggest issue is the internet's main purpose in life, which is an openly accessible network with everyone able to talk to everyone else. Thus, the internet's main *advantage i*s now becoming its biggest *disadvantage*.

Combinatorial Testing

A NIST (National Institute of Standards and Technology, USA) paper tackles the problems of software reliability and cyber security in an article outlining the concept of *combinatorial testing*. Combinatorial testing is a method that can reduce cost and increase the effectiveness of software testing for many

[2] The survey covered 600 IT and security executives across 14 countries, including the USA.
[3] This can have a massive financial effect on some companies.

applications. The key insight underlying this form of testing is that not every parameter contributes to every failure and most failures are caused by interactions between relatively few parameters:

COMBINATORIAL TESTING FOR CYBERSECURITY AND RELIABILITY
http://csrc.nist.gov/publications/nistbul/itlbul2016_05.pdf

Also, see the references within the document above for more information on this topic plus areas of use.

First Line of Defense

The Corero papers below are useful adjuncts to the ones at the end of this article which expand upon the problem and its effects. The papers outline solution areas to mitigate these attacks, suggesting the user side of the firewall defense as the location for your cybercrime redoubt.

First Line of Defense to Protect Critical Infrastructure
http://csrc.nist.gov/cyberframework/rfi_comments/040813_corero.pdf

Corero Network Security First Line of Defense Overview
http://www.dotforce.it/wp-content/uploads/2014/08/Corero_First_Line_of_Defense_Solution_Overview_140916.pdf

Summary

Cyber attacks are here to stay and are not only breeding like rabbits but are growing into something bigger and stronger. The biggest problem in this area is the openness of the internet and the relatively easy access to any services using it. I am baffled as to why a top secret system such as the US DoD and other militarily sensitive sites are attached to such a wide-open facility.

Despite today's hardware and software being highly reliable, the problem of prolonged or short but damaging *outages* is not going away. Human finger trouble, accidental or deliberate, and cyber criminals are upping the ante in the availability stakes; and unless the IT world matches it, it will have to fold its hands.

I have some half-baked ideas about ways to approach the problem, though not a specifiable solution; and they are based on the sports principle that attack is the best form of defense. I may specify it further one day.

References

1. *High Availability IT Services* [Dec 24 2014]
https://www.crcpress.com/High-Availability-IT-Services/Critchley/9781482255904

2. *High Performance IT Services* [due July 16]
https://www.crcpress.com/High-Performance-IT-Services/Critchley/9781498769198

3. *Trust and Trustworthy Computing: Third International Conference, TRUST 2010*
[edited by Alessandro Acquisti, Sean Smith, Ahmad-Reza Sadeghi]
https://books.google.co.uk/books?id=H7ZtCQAAQBAJ&pg=PA339&dq=downtime+cyber+attacks&hl=en&sa=X&ved=0ahUKEwj25Kjmt9vMAhVlJ8AKHa_PAP4Q6AEIRjAD#v=onepage&q=downtime%20cyber%20attacks&f=false

4. *Victimology*
https://books.google.co.uk/books?isbn=0323296386
[William G. Doerner, Steven P. Lab - 2014]